Results 1 - 20 of 20

Sort by relevance in expanded form

Save results to a Binder

1 Electronic Signature Formats for long term electronic signatures

D. Pinkas, J. Ross, N. Pope

September 2001 Electronic Signature Formats for long term electronic signatures

Publisher: RFC Editor

Full text available: Txt (175.89 KB) Additional Information: full citation, abstract, cited by

Bibliometrics: Downloads (6 Weeks): 3, Downloads (12 Months): 8, Citation Count: 1

This document defines the format of an electronic signature that can remain valid over long periods. This includes evidence as to its validity even if the signer or verifying party later attempts to deny (i.e., repudiates the validity of the signature).

2 Policy Requirements for Time-Stamping Authorities (TSAs)

D. Pinkas, N. Pope, J. Ross

November 2003 Policy Requirements for Time-Stamping Authorities (TSAs)

Publisher: RFC Editor

Full text available: Txt (92.94 KB) Additional Information: full citation, abstract

Bibliometrics: Downloads (6 Weeks): 0, Downloads (12 Months): 1, Citation Count: 1

This document defines requirements for a baseline time-stamp policy for Time-Stamping Authorities (TSAs) issuing time-stamp tokens, supported by public key certificates, with an accuracy of one second or better. A TSA may define its own policy which ...

Found **20** of **1,352,536**

3 Long-term trusted preservation service using service interaction protocol and evidence records

Aleksej Jerman Blaˇ, Toma Klobuˇar, Borka Donova Jerman

March 2007 **Computer Standards & Interfaces** , Volume 29 Issue 3

Publisher: Elsevier Science Publishers B. V.

Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Citation Count: 0

The e-business and e-government processes demand to prove the existence of data at a specific point of time and to demonstrate the integrity of the data since that time during long-term periods is becoming of utmost importance. An approach and a solution ...

Keywords: Authenticity, Authority, Electronic archive, Evidence, Integrity, Long-term, Preservation, Protocol, Record, Trust, Validity

4 On the performance, feasibility, and use of forward-secure signatures

Eric Cronin, Sugih Jamin, Tal Malkin, Patrick McDaniel

October 2003 **CCS '03:** Proceedings of the 10th ACM conference on Computer and communications security

Publisher: ACM Request Permissions

Full text available: Pdf (386.51 KB) Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 10, Downloads (12 Months): 71, Citation Count: 6

Forward-secure signatures (FSSs) have recently received much attention from the cryptographic theory community as a potentially realistic way to mitigate many of the difficulties digital signatures face with key exposure. However, no previous works have ...

Keywords: digital signatures, forward-secure signatures

5 Independent Data Unit Protection Generic Security Service Application Program Interface (IDUP-GSS-API)

C. Adams

December 1998 Independent Data Unit Protection Generic Security Service Application Program Interface (IDUP-GSS-API)

Publisher: RFC Editor

Full text available: Txt (156.07 KB) Additional Information: full citation, cited by

Bibliometrics: Downloads (6 Weeks): 0, Downloads (12 Months): 1, Citation Count: 1

6 Electronic Signature Policies

J. Ross, D. Pinkas, N. Pope

September 2001 Electronic Signature Policies

Publisher: RFC Editor

Full text available: Txt (95.51 KB) Additional Information: full citation, abstract

Bibliometrics: Downloads (6 Weeks): 0, Downloads (12 Months): 3, Citation Count: 0

This document defines signature policies for electronic signatures. A signature policy is a set of rules for the creation and validation of an electronic signature, under which the validity of signature can be determined. A given legal/contractual context ...

7 Improving secure long-term archival of digitally signed documents

Carmela Troncoso, Danny De Cock, Bart Preneel

October 2008 **StorageSS '08:** Proceedings of the 4th ACM international workshop on Storage security and survivability

Publisher: ACM Request Permissions

Full text available: Pdf (977.50 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 13, Downloads (12 Months): 122, Citation Count: 1

Long-term archival of signed documents presents specific challenges that do not need to be considered in short-term storage systems. In this paper we present a Secure Long-Term Archival System (SLTAS) that protects, in a verifiable way, the validity ...

Keywords: digitally signed documents, retimestamping, secure long-term archiving

8 Legal deposit of digital publications: a review of research and development activity

Adrienne Muir

January 2001 **JCDL '01:** Proceedings of the 1st ACM/IEEE-CS joint conference on Digital libraries

Publisher: ACM Request Permissions

Full text available: Pdf (206.75 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 3, Downloads (12 Months): 42, Citation Count: 0

There is a global trend towards extending legal deposit to include dig ital publications in order to maintain comprehensive national archives. However, including digital publications in legal deposit regulation is not enough to ensure the long-term preservation ...

Keywords: digital preservation, digital publications, legal deposit

9 Efficient signature schemes supporting redaction, pseudonymization, and data deidentification

Stuart Haber, Yasuo Hatano, Yoshinori Honda, William Horne, Kunihiko Miyazaki, Tomas Sander, Satoru Tezoku, Danfeng Yao

March 2008 **ASI ACCS '08:** Proceedings of the 2008 ACM symposium on Information, computer and communications security

Publisher: ACM Request Permissions

Full text available: Pdf (296.30 KB) Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 17, Downloads (12 Months): 134, Citation Count: 1

In this paper we give a new signature algorithm that allows for controlled changes to the signed data. The change operations we study are removal of subdocuments (redaction), pseudonymization, and gradual deidentification of hierarchically structured ...

Keywords: audit logs, data integrity, data privacy, digital signatures, pseudonyms, redaction

10 A remote personal device management framework based on SyncML DM specifications

Hailiang Mei, Johan Lukkien

May 2005 **MDM '05:** Proceedings of the 6th international conference on Mobile data management

Publisher: ACM Request Permissions

Full text available: Pdf (335.13 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 13, Downloads (12 Months): 53, Citation Count: 1

This paper describes a new design of the remote device management (RDM) framework, which is suited to personal devices. Once this Remote Personal Device Management (RPDM) framework is enabled, parties like manufacturing companies, service providers, ...

Keywords: RPDM, SyncML DM, access control, privacy, remote device management, security

11 Image retrieval: Ideas, influences, and trends of the new age

Ritendra Datta, Dhiraj Joshi, Jia Li, James Z. Wang

April 2008 **Computing Surveys (CSUR)** , Volume 40 Issue 2

Publisher: ACM Request Permissions

Full text available: Pdf (2.81 MB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 307, Downloads (12 Months): 3022, Citation Count: 38

We have witnessed great interest and a wealth of promise in content-based image retrieval as an emerging technology. While the last decade laid foundation to such promise, it also paved the way for a large number of new techniques and systems, got many ...

Keywords: Content-based image retrieval, annotation, learning, modeling, tagging

12 Tamper detection in audit logs

Richard T. Snodgrass, Shilong Stanley Yao, Christian Collberg

August 2004 **VLDB '04: Proceedings of the Thirtieth international conference on Very large data bases - Volume 30** , Volume 30

Publisher: VLDB Endowment

Full text available: Pdf (186.30 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 5, Downloads (12 Months): 30, Citation Count: 4

Audit logs are considered good practice for business systems, and are required by federal regulations for secure systems, drug approval data, medical information disclosure, financial records, and electronic voting. Given the central role of audit logs, ...

13 Minimal information disclosure with efficiently verifiable credentials

David Bauer, Douglas M. Blough, David Cash

October 2008 **DIM '08:** Proceedings of the 4th ACM workshop on Digital identity management

Publisher: ACM Request Permissions

Full text available: Pdf (434.34 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 8, Downloads (12 Months): 116, Citation Count: 2

Public-key based certificates provide a standard way to prove one's identity, as attested by some certificate authority (CA). However, plain certificates provide a binary identification: either the whole identity of the subject is known, or nothing is ...

Keywords: PKI, credential, hash-tree, identity assertion, identity management, merkle tree, privacy

14 Large-scale IP traceback in high-speed internet: practical techniques and information-theoretic foundation

Minho Sung, Jun Xu, Jun Li, Li Li

December 2008 **IEEE/ ACM Transactions on Networking (TON)** , Volume 16 Issue 6

Publisher: IEEE Press Request Permissions

Full text available: Pdf (775.60 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 28, Downloads (12 Months): 89, Citation Count: 0

Tracing attack packets to their sources, known as IP traceback, is an important step to counter distributed denial-of-service (DDoS) attacks. In this paper, we propose a novel packet logging based (i.e., hash-based) traceback scheme that requires an ...

Keywords: IP traceback, distributed denial-of-service attacks, information theory, network security

15 Accountable certificate management using undeniable attestations

Ahto Buldas, Peeter Laud, Helger Lipmaa

November 2000 **CCS '00:** Proceedings of the 7th ACM conference on Computer and communications security

Publisher: ACM  Request Permissions

Full text available:  Pdf (469.67 KB) Additional Information: full citation, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 2, Downloads (12 Months): 37, Citation Count: 14

Keywords: accountable certificate management, attesters, authenticated search trees, long-term authenticity, non-repudiation, public-key infrastructure, search trees, time-stamping

16 New techniques for ensuring the long term integrity of digital archives

Sangchul Song, Joseph JaJa

May 2007 **dg.o '07:** Proceedings of the 8th annual international conference on Digital government research: bridging disciplines & domains

Publisher: Digital Government Research Center

Full text available:  Pdf (607.08 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 5, Downloads (12 Months): 77, Citation Count: 0

A large portion of the government, business, cultural, and scientific digital data being created today needs to be archived and preserved for future use of periods ranging from a few years to decades and sometimes centuries. A fundamental requirement ...

Keywords: data integrity, digital archives, integrity audits, linked hashing

17 A countable and time-bound password-based user authentication scheme for the applications of electronic commerce

Iuon-Chang Lin, Chin-Chen Chang

April 2009 **Information Sciences: an International Journal** , Volume 179 Issue 9

Publisher: Elsevier Science Inc.

Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Citation Count: 0

In this paper, we propose a secure and efficient user authentication scheme with countable and time-bound features. The countable feature is to limit the use to a certain number of times, which means that the users are able to successfully log into the ...

Keywords: Electronic commerce, Password-based user authentication, Quadratic residue

18 Remote Attestation on Legacy Operating Systems With Trusted Platform Modules

Dries Schellekens, Brecht Wyseur, Bart Preneel

February 2008 **Electronic Notes in Theoretical Computer Science (ENTCS)** , Volume 197 Issue 1

Publisher: Elsevier Science Publishers B. V.

Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Citation Count: 0

A lot of progress has been made to secure network communication, e.g., through the use of cryptographic algorithms. However, this offers only a partial solution as long as the communicating end points still suffer from security problems. A number of ...

Keywords: attestation, remote software authentication, timed execution, trusted platform module

19 Eliminating counterevidence with applications to accountable certificate management

Ahto Buldas, Peeter Laud, Helger Lipmaa

September 2002 **Journal of Computer Security** , Volume 10 Issue 3

Publisher: IOS Press

Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Citation Count: 5

This paper presents a method to increase the accountability of certificate management by making it intractable for the certification authority (CA) to create contradictory statements about the validity of a certificate. The core of the method is a new ...

Keywords: accountable certificate management, attesters, authenticated search trees, long-term authenticity, non-repudiation, public-key infrastructure, search trees, time-stamping

20 Classification of Hash Functions Suitable for Real-Life Systems

Yasumasa Hirai, Takashi Kurokawa, Shin'ichiro Matsuo, Hidema Tanaka, Akihiro Yamamura

January 2008 **IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences** , Volume E91-A Issue 1

Publisher: Oxford University Press

Additional Information: full citation, abstract, references

Bibliometrics: Downloads (6 Weeks): n/a, Downloads (12 Months): n/a, Citation Count: 0

Cryptographic hash functions have been widely studied and are used in many current systems. Though much research has been done on the security of hash functions, system designers cannot determine which hash function is most suitable for a particular ...

Keywords: hash function, security